REMARKS

In view of the following discussion, the Applicants submit that none of the claims now pending in the application is directed to non-statutory subject matter under 35 U.S.C. §101, anticipated under the provisions of 35 U.S.C. §102, or obvious under the provisions of 35 U.S.C. §103. Thus, the Applicants believe that all of these claims are in allowable form.

I. REJECTION OF CLAIMS 10, 12, AND 13 UNDER 35 U.S.C. §101

Claims 10, 12, and 13 stand rejected as being allegedly directed to non-statutory subject matter. Specifically, the Examiner alleges that "the applicant has not shown that the computer readable medium [recited in claims 10, 12, and 13] is hardware." In response, the Applicants have amended independent claims 10 and 12 to recite a "computer readable storage medium," replacing a "computer readable medium." Claim 13 has been cancelled without prejudice. In light of these amendments, the Applicants respectfully submit that claims 10 and 12 fully satisfy the requirements of 35 U.S.C. §101. Accordingly, the Applicants respectfully request that the rejection under 35 U.S.C. §101 be withdrawn.

II. REJECTION OF CLAIMS 1-2, 4-5, AND 10-13 UNDER 35 U.S.C. § 102

Claims 1-2, 4-5, and 10-13 stand rejected as being anticipated by the Purtell et al. patent (U.S. 6,950,947, issued September 27, 2005, hereinafter "Purtell"). In response, the Applicants have amended independent claims 1, 4-5, and 10-12 in order to more clearly recite aspects of the present invention. Claim 13 has been cancelled without prejudice, as discussed above.

Particularly, the Examiner's attention is directed to the fact that Purtell fails to disclose or suggest a method for correlating sensors in an intrusion detection system by adjusting a belief state of a first sensor based on a belief state of a second sensor, where the adjustment improves the sensitivity of the first sensor to suspicious activity (*e.g.*, attempted communications with a nonexistent services or resources) and/or reduces alarms generated by erroneous transactions, as claimed in Applicants' independent claims 1, 4, 5, and 10 - 12.

By contrast, Purtell discloses a set of peer firewalls/proxy servers that share

information about transmission control protocol (TCP) control state in order to enhance the efficiency of TCP throughput in a network. Purtell says nothing about the need to monitor the network for suspected intrusions, *e.g.*, by using an intrusion detection system, as claimed by the Applicants in independent claims 1, 4, 5, and 10 - 12. A firewall, which filters data before it can reach the network (*See*, *e.g.*, column 1, lines 33-41 of Purtell: "A firewall typically filters network packets received from the external network to determine whether to forward them to their destination on the internal network," emphasis added), is not the same as an intrusion detection system, which identifies potential intrusions based on analysis of data that has already entered the network. Thus, a firewall may be considered an intrusion prevention system, but not an intrusion detection system.

Moreover, as discussed above, Purtell is directed to a method for improving throughput between firewalls and servers by sharing TCP connection state data. For instance, by sharing information concerning congestion, round trip time, and other state components affecting packet transmission to/from a particular server, a connection between a firewall and the server may be initiated in a manner that maximizes data transfer speed (*See*, *e.g.*, Purtell, column 8, lines 44-53). Purtell fails to disclose or suggest detecting suspicious activity in a network or generating alarms in response to such detections. In fact, the words "suspicious" and "alarm" do not even appear in the disclosure of Purtell.

Thus, Purtell fails to disclose or suggest a method for correlating sensors in an intrusion detection system by adjusting a belief state of a first sensor based on a belief state of a second sensor, where the adjustment improves the sensitivity of the first sensor to suspicious activity (*e.g.*, attempted communications with a nonexistent services or resources) and/or reduces alarms generated by erroneous transactions, as claimed in Applicants' independent claims 1, 4, 5, and 10 - 12. Specifically, Applicants' claims 1, 4, 5, and 10 - 12 positively recite:

1. A method for correlating a first sensor to a second sensor in an intrusion detection system, the first sensor and the second sensor each maintaining belief regarding a resource or service monitored by the intrusion detection system, the method comprising the steps of:

(a) transmitting to the first sensor information about a belief state of the

second sensor, said belief state of the second sensor indicating a state of at least one system resource or service directly monitored by the second sensor; and

(b) adjusting a belief state of the first sensor, said belief state of the first sensor indicating a state of at least one system resource or service directly monitored by the first sensor, the adjusting based at least in part on the belief state of the second sensor, so that a sensitivity of the first sensor to suspicious activity in the intrusion detection system is improved. (Emphasis added)

4. A method for reducing false alarms generated by an intrusion detection system when a monitored resource is degraded or compromised, the intrusion detection system having a first sensor and a second sensor each maintaining belief regarding a state of a resource monitored by the intrusion detection system, the method comprising the steps of:

(a) transmitting to the first sensor all or part of a belief of the second sensor regarding an apparent normal, degraded or compromised state of a resource directly monitored by the second sensor; and

(b) adjusting a belief state of the first sensor, said belief state of the first sensor indicating an apparent normal, degraded or compromised state of a resource directly monitored by the first sensor, so that an erroneous transaction with the degraded or compromised resource does not generate an alarm in the intrusion detection system. (Emphasis added)

5. A method for enhancing a sensitivity of an intrusion detection system that monitors a plurality of computer system resources, the intrusion detection system having a first sensor and a second sensor each maintaining belief regarding a service monitored by the intrusion detection system, the method comprising the steps of:

(a) transmitting to the first sensor all or part of a belief state of the second sensor regarding an existence or validity of services supported on computer system resources directly monitored by the second sensor; and

(b) adjusting a belief state of the first sensor, said belief state of the first sensor indicating an existence or validity of services supported on computer system resources directly monitored by the first sensor, so that an attempted communication with a nonexistent system service or resource appears suspicious to the intrusion detection system. (Emphasis added)

10. A computer readable storage medium containing an executable program for correlating a first sensor to a second sensor in an intrusion detection system, the first sensor and the second sensor each maintaining belief regarding a resource or service monitored by the intrusion detection system, where the program performs the steps of:

(a) transmitting to the first sensor information about a belief state of the second sensor, said belief state of the second sensor indicating a state of at least one system resource or service directly monitored by the second sensor; and

(b) adjusting a belief state of the first sensor, said belief state of the first sensor indicating a state of at least one system resource or service directly monitored

by the first sensor, the adjusting based at least in part on the belief state of the second sensor, so that a sensitivity of the first sensor to suspicious activity in the intrusion detection system is improved. (Emphasis added)

11. A computer readable storage medium containing an executable program for reducing false alarms generated by an intrusion detection system when a monitored resource is degraded or compromised, the intrusion detection system having a first sensor and a second sensor each maintaining belief regarding a state of a resource monitored by the intrusion detection system, where the program performs the steps of:

(a) transmitting to the first sensor all or part of a belief of the second sensor regarding an apparent normal, degraded or compromised state of a resource directly monitored by the second sensor; and

(b) adjusting a belief state of the first sensor, said belief state of the first sensor indicating an apparent normal, degraded or compromised state of a resource directly monitored by the first sensor, so that an erroneous transaction with the degraded or compromised resource does not generate an alarm in the intrusion detection system. (Emphasis added)

12. A computer readable storage medium containing an executable program for enhancing a sensitivity of an intrusion detection system that monitors a plurality of computer system resources, the intrusion detection system having a first sensor and a second sensor each maintaining belief regarding a service monitored by the intrusion detection system, where the program performs the steps of:

(a) transmitting to the first sensor all or part of a belief state of the second sensor regarding an existence or validity of services supported on computer system resources directly monitored by the second sensor; and

(b) adjusting a belief state of the first sensor, said belief state of the first sensor indicating an existence or validity of services supported on computer system resources directly monitored by the first sensor, so that an attempted communication with a nonexistent system service or resource appears suspicious to the intrusion detection system. (Emphasis added)

As discussed above, Purtell fails to disclose or suggest a method for correlating sensors in an intrusion detection system by adjusting a belief state of a first sensor based on a belief state of a second sensor, where the adjustment improves the sensitivity of the first sensor to suspicious activity (*e.g.*, attempted communications with a nonexistent services or resources) and/or reduces alarms generated by erroneous transactions, as claimed in Applicants' independent claims 1, 4, 5, and 10 - 12. Therefore, the Applicants submit that independent claims 1, 4, 5, and 10 - 12 fully satisfy the requirements of 35 U.S.C. §102 and are patentable thereunder.

Dependent claim 2 depends from claim 1 and recites additional features

therefore. As such, and for at least the same reasons set forth above, the Applicants submit that claim 2 is not anticipated by the teachings of Purtell. Moreover, Purtell fails to teach or suggest the method of claim 1, wherein the first and second sensors are different types of sensors, as recited by Applicants' claim 2. By contrast, Purtell teaches a system in which devices of the same type (*i.e.*, firewalls) share data (TCP control blocks). There is no suggestion anywhere in Purtell that the shared data is provided to any devices other than the firewalls. The portion of Purtell that the Examiner cites to teach the feature of first and second sensors that are different types of sensors at best teaches that multiple firewalls may be connected together by an internal network. The cited portion of Purtell does not teach that the multiple firewalls are different types of devices. Therefore, the Applicants submit that dependent claim 2 also fully satisfies the requirements of 35 U.S.C. §102 and is patentable thereunder.

III. REJECTION OF CLAIM 3 UNDER 35 U.S.C. § 103

Claim 3 stands rejected as being unpatentable over Purtell in view of the Timm patent (U.S. 5,440,498, hereinafter "Timm"). The Applicants respectfully traverse the rejection.

As discussed above, Purtell does not teach or even suggest a method for correlating sensors in an intrusion detection system by adjusting a belief state of a first sensor based on a belief state of a second sensor, where the adjustment improves the sensitivity of the first sensor to suspicious activity (*e.g.*, attempted communications with a nonexistent services or resources) and/or reduces alarms generated by erroneous transactions, as claimed in Applicants' independent claim 1, from which claim 3 depends. Applicants' claim 1 has been recited above. Timm does not bridge this gap in the teachings of Purtell. Purtell and Timm, singularly or in any permissible combination, thus fail to teach, suggest all of the features of Applicants' independent claim 1. Therefore, the Applicants submit that independent claim 1 fully satisfies the requirements of 35 U.S.C. §103 and is patentable thereunder.

Dependent claim 3 depends from claim 1 and recites additional features therefore. As such, and for at least the same reasons set forth above, the Applicants submit that claim 3 is not made obvious by the teachings of Purtell in view of Timm. Therefore, the Applicants submit that dependent claim 3 also fully satisfies the

requirements of 35 U.S.C. §103 and is patentable thereunder.

IV. CONCLUSION

Thus, the Applicants submit that all of the presented claims fully satisfy the requirements of 35 U.S.C. §101, 35 U.S.C. §102 and 35 U.S.C. §103. Consequently, the Applicants believe that all of these claims are presently in condition for allowance. Accordingly, both reconsideration of this application and its swift passage to issue are earnestly solicited.

If, however, the Examiner believes that there are any unresolved issues requiring the issuance of a final action in any of the claims now pending in the application, it is requested that the Examiner telephone Mr. Kin-Wah Tong, Esq. at (732) 530-9404 so that appropriate arrangements can be made for resolving such issues as expeditiously as possible.

Respectfully submitted,

5/9/08
Date

Kin-Wah Tong, Attorney
Reg. No. 39,400
(732) 530-9404

Patterson & Sheridan, LLP
595 Shrewsbury Avenue
Shrewsbury, New Jersey 07702